Richard A. Jacobsen (RJ5136)
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, New York 10019
Telephone: (212) 506-5000
Facsimile: (212) 506-5151

Gabriel M. Ramsey
(admitted *pro hac vice*)
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, California 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

Attorneys for Plaintiffs
MICROSOFT CORPORATION,
FS-ISAC, INC. and NATIONAL AUTOMATED
CLEARING HOUSE ASSOCIATION

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORP., FS-ISAC, INC., and NATIONAL AUTOMATED CLEARING HOUSE ASSOCIATION,

Plaintiffs

v.

JOHN DOES 1-39 D/B/A Slavik, Monstr, IOO, Nu11, nvidiag, zebra7753, lexa_Mef, gss, iceIX, Harderman, Gribodemon, Aqua, aquaSecond, it, percent, cp01, hct, xman, Pepsi, miami, miamibc, petr0vich, Mr. ICQ, Tank, tankist, Kusunagi, Noname, Lucky, Bashorg, Indep, Mask, Enx, Benny, Bentley, Denis Lubimov, MaDaGaSka, Vkontake, rfcid, parik, reronic, Daniel, bx1, Daniel Hamza, Danielbx1, jah, Jonni, jtk, D frank, duo, Admin2010, h4x0rdz, Donsft, mary.J555, susanneon, kainehabe, virus_e_2003, spanishp, sere.bro, muddem, mechan1zm, vlad.dimitrov, jheto2002, sector.exploits AND JabberZeus Crew, AND YEVHEN KULIBABA AND YURIY KONOVALENKO, CONTROLLING COMPUTER BOTNETS THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS,

Defendants.

Hon. Sterling Johnson, Jr.

Case No. 12-cv-01335 (SJ/RLM)

AMENDED COMPLAINT

Plaintiffs MICROSOFT CORP. ("Microsoft"), FINANCIAL SERVICES – INFORMATION SHARING AND ANALYSIS CENTER, INC. ("FS-ISAC") and the NATIONAL AUTOMATED CLEARING HOUSE ASSOCIATION ("NACHA"), hereby complain and allege that JOHN DOES 1-39 ("John Does" or "Doe Defendants"), Yevhen Kulibaba and Yuriy Konovalenko (all, collectively the "Defendants") are controlling a worldwide, illegal computer network, collectively known as the "Zeus Botnets," comprised of end-user computers connected to the Internet that Defendants have infected with malicious software. Defendants have used the Zeus Botnets to infect over 13 million computers on the Internet, which were then used to steal over $100 million during the past five years. Defendants control the Zeus Botnets through a sophisticated command and control infrastructure hosted at and operated through Internet domains set forth at Appendix A and the Internet file paths set forth at Appendix C to this Complaint (hereinafter the "Harmful Domains") and the Internet Protocol addresses set forth at Appendix B to this Complaint (hereinafter the "Harmful IP Addresses") (herein collectively referred to as the "Harmful Domains and IP Addresses"), as follows:

NATURE OF ACTION

1. This is an action based upon: the Computer Fraud and Abuse Act (18 U.S.C. § 1030); CAN-SPAM Act (15 U.S.C. § 7704); Electronic Communications Privacy Act (18 U.S.C. § 2701); trademark infringement under the Lanham Act (15 U.S.C. § 1114), false designation of origin under the Lanham Act (15 U.S.C. § 1125(a)); trademark dilution under the Lanham Act (15 U.S.C. § 1125(c)); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962(c)); unjust enrichment; trespass to chattels; and common law conversion. Plaintiffs seek injunctive and other equitable relief and damages against Defendants for their creation, control, maintenance, and ongoing use of the Zeus Botnets, which have caused and continue to cause irreparable injury to Plaintiffs, Plaintiffs' customers and members, and the general public.

THE PARTIES

2. Plaintiff Microsoft Corp. is a corporation duly organized and existing under the

laws of the State of Washington, having its headquarters and principal place of business in Redmond, Washington. Microsoft is a leading provider of technology products and services, including computer software, Internet services, websites and email services.

3. Plaintiff FS-ISAC, Inc. is a non-profit corporation duly organized and existing under the laws of Delaware, having its headquarters and principal place of business in Reston, Virginia. FS-ISAC is a membership organization comprised of 4,400 organizations including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, payment processors, and over 20 trade associations representing the majority of the U.S. financial services sector. FS-ISAC represents the interests of its financial services industry members in combating and defending against cyber threats that pose risk and loss to the industry.

4. Plaintiff National Automated Clearing House Association is a non-profit corporation duly organized and existing under the laws of Delaware, having its principal place of business in Herndon, Virginia. NACHA manages the development, administration, and governance of the ACH Network, the backbone for the electronic movement of money and data, and represents more than 10,000 financial institutions via 17 regional payments associations and direct membership.

5. Plaintiffs are informed and believe and thereupon allege that John Doe 1 is the creator of the "Zeus" botnet code that, along with the "Ice-IX" and "SpyEye" botnet codes, comprise the Zeus Botnets. John Doe 1 goes by the aliases "Slavik," "Monstr," "IOO" and/or "Nu11" and may be contacted at messaging address bashorg@talking.cc.

6. Plaintiffs are informed and believe and thereupon allege that John Doe 2 is the creator of the "Ice-IX" botnet code that, along with the "Zeus" and "SpyEye" botnet codes, comprise the Zeus Botnets. John Doe 2 goes by the aliases "zebra7753," "lexa_mef," "gss," and "iceIX" and may be contacted at Jabber messaging address iceix@secure-jabber.biz and ICQ messaging address "610875708."

7. Plaintiffs are informed and believe and thereupon allege that John Doe 3 is the creator of the "SpyEye" botnet code that, along with the "Zeus" and "Ice-IX" botnet codes,

comprise the Zeus Botnets. John Doe 3 goes by the aliases "Harderman" or "Gribodemon" and may be contacted at email and messaging addresses shwark.power.andrew@gmail.com, johnlecun@gmail.com, gribodemon@pochta.ru, glazgo-update-notifier@gajim.org, and gribo-demon@jabber.ru.

8. Plaintiffs are informed and believe and thereupon allege that John Does 1 through 3, as creators of the malicious botnet code, have acted in concert with John Does 4 through 39 who have purchased, developed and/or sold such botnet code, and are currently operating or have contributed to the operation of the Zeus Botnets.

9. Plaintiffs are informed and believe and thereupon allege that John Doe 4 goes by the aliases "Aqua," "aquaSecond," "it," "percent," "cp01," "hct," "xman," and "Pepsi" and may be contacted at messaging addresses aqua@incomeet.com and "637760688." Upon information and belief, John Doe 4 recruits money mules and uses them to cash out stolen account credentials, and operates the Zeus Botnets to compromise account credentials.

10. Plaintiffs are informed and believe and thereupon allege that John Doe 5 goes by the aliases "miami" and "miamibc" and may be contacted at messaging addresses miami@jabbluisa.com, um@jabbim.com, and hof@headcounter.org. Upon information and belief, John Doe 5 is a developer of "web inject" logic for the Zeus Botnets and has been called on by other Doe Defendants in this case to develop web inject code for Zeus Botnet configuration files (*e.g.* injecting additional website form fields, such as ATM card number, pin, etc, as described further below).

11. Plaintiffs are informed and believe and thereupon allege that John Doe 6 goes by the alias "petr0vich" and may be contacted at email and messaging addresses theklutch@gmail.com, niko@grad.com, Johnny@guru.bearin.donetsk.ua, petr0vich@incomeet.com and 802122. Upon information and belief, John Doe 6 is a primary network administrator for other John Doe defendants in this case, handling most of the tasks relating to Zeus hosting and operations.

12. Plaintiffs are informed and believe and thereupon allege that John Doe 7 goes by

the alias "Mr ICQ" and may be contacted at messaging address mricq@incomeet.com. Upon information and belief, John Doe 7 is one of the actors in Defendants' organization who handles incoming notifications of newly compromised victim information. Upon further information and belief, John Doe 7 is also connected to underground electronic currency exchange services.

13. Plaintiffs are informed and believe and thereupon allege that John Doe 8 goes by the alias "Tank" and "tankist" and may be contacted at email and messaging addresses T4ank@ua.fm, tank@incomeet.com and 366666. Upon information and belief, John Doe 8 works closely with John Doe 6 and is involved in cashing out stolen credentials.

14. Plaintiffs are informed and believe and thereupon allege that John Doe 9 goes by the alias "Kusunagi." Upon information and belief, John Doe 9 is involved in writing and obtaining web inject code. Upon further information and belief, John Doe 9 can likely be contacted at email and messaging addresses T4ank@ua.fm, tank@incomeet.com and 366666.

15. Plaintiffs are informed and believe and thereupon allege that John Doe 10 goes by the alias "Noname." Upon information and belief, John Doe 10 is associated with John Doe 4, operates the Zeus Botnets and can likely be contacted at aqua@incomeet.com and "637760688."

16. Plaintiffs are informed and believe and thereupon allege that John Doe 11 goes by the aliases "Lucky" and "Bashorg" and may be contacted at messaging address "647709019." Upon information and belief, John Doe 11 is a Zeus code vendor and has provided cashiering functions (e.g. initiator of ACH/wire transaction) to other Defendants.

17. Plaintiffs are informed and believe and thereupon allege that John Doe 12 goes by the alias "Indep." Upon information and belief, John Doe 12 is associated with John Does 1, 8 and 11 and can likely be contacted at T4ank@ua.fm, tank@incomeet.com and "366666," "647709019." Upon further information and belief, John Doe 12 operates the latest versions of the Zeus Botnets.

18. Plaintiffs are informed and believe and thereupon allege that John Doe 13 goes by the alias "Mask." Upon information and belief, John Doe 13 is involved in Defendants' money mule operations.

19. Plaintiffs are informed and believe and thereupon allege that John Doe 14 goes by the alias "Enx." Upon information and belief, John Doe 14 is involved in Defendants' money mule operations.

20. Plaintiffs are informed and believe and thereupon allege that John Doe 15 goes by the aliases "Benny," "Bentley," "Denis Lubimov," "MaDaGaSkA," and "Vkontake" and may be contacted at email and messaging addresses getready@safebox.ru, john.mikle@ymail.com, alexeysafin@yahoo.com, moscow.berlin@yahoo.com, cruelintention@email.ru, bind@email.ru, firstmen17@rambler.ru, benny@jabber.cz, "77677776," "76777776," "173094207," and "45677777." Upon information and belief, John Doe 15 specializes in money mule recruitment of young people going to the U.S., or already in the U.S., on a J1 student visa. Upon further information and belief, John Doe 15 advertizes a cash-out service known as "Hot Spot" and is believed to work with John Doe 6 on a regular basis.

21. Plaintiffs are informed and believe and thereupon allege that John Doe 16 goes by the alias "rfcid." Upon information and belief, John Doe 16 has purchased and used Zeus Botnet code.

22. Plaintiffs are informed and believe and thereupon allege that John Doe 17 goes by the alias "parik." Upon information and belief, John Doe 17 has purchased and used Zeus Botnet code.

23. Plaintiffs are informed and believe and thereupon allege that John Doe 18 goes by the alias "reronic." Upon information and belief, John Doe 18 was involved in testing and using the merged "Zeus/SpyEye" code.

24. Plaintiffs are informed and believe and thereupon allege that John Doe 19/20 goes by the aliases "Daniel," "bx1," "Daniel Hamza" and "Danielbx1" and may be contacted at messaging email and messaging addresses "565359703," airlord1988@gmail.com, bx1@hotmail.com, i_amhere@hotmail.fr, daniel.h.b@universityof sutton.com, princedelune@hotmail.fr, bx1_@msn.com, danibx1@hotmail.fr, and danieldelcore@hotmail.com. Upon information and belief, John Doe 19/20 has purchased and

used the Zeus/SpyEye code.

25. Plaintiffs are informed and believe and thereupon allege that John Doe 21 goes by the alias "jah." Upon information and belief, John Doe 21 is associated with John Doe 20. Upon further information and belief, John Doe 21 was involved with the development of the Zeus/SpyEye code.

26. Plaintiffs are informed and believe and thereupon allege that Yevhen Kulibaba (John Doe 22) goes by the alias "Jonni." Upon information and belief, Yevhen Kulibaba resides in the United Kingdom, may be contacted through counsel in Croydon, United Kingdom, and is associated with Yuriy Konovalenko and John Doe 4. Upon further information and belief, Yevhen Kulibaba has specialized in money mule recruitment in the UK.

27. Plaintiffs are informed and believe and thereupon allege that Yuriy Konovalenko (John Doe 23/24) goes by the alias "jtk." Upon information and belief, Yuriy Konovalenko resides in the United Kingdom, may be contacted through counsel in London, United Kingdom, and is associated with Yevhen Kulibaba and John Does 4 and 6. Upon further information and belief, Yuriy Konovalenko has specialized in money mule recruitment in the UK.

28. Plaintiffs are informed and believe and thereupon allege that John Doe 25 goes by the alias "D frank" and may be contacted at messaging addresses d.frank@jabber.jp and d.frank@0nl1ne.at. Upon information and belief, John Doe 25 is involved in hosting Zeus Botnet code.

29. Plaintiffs are informed and believe and thereupon allege that John Doe 26 goes by the alias "duo" and may be contacted at messaging address duo@jabber.cn. Upon information and belief, John Doe 26 is involved in hosting Zeus Botnet code.

30. Plaintiffs are informed and believe and thereupon allege that John Doe 27 goes by the alias "Admin2010" and may be contacted at email addresses fering99@yahoo.com and secustar@mail.ru. Upon information and belief, John Doe 27 is involved in purchasing and using the Zeus Botnet code.

31. Plaintiffs are informed and believe and thereupon allege that John Doe 28 goes by

the alias "h4x0rdz" and may be contacted at email address h4x0rdz@hotmail.com. Upon information and belief, John Doe 28 is involved in purchasing and using the Zeus/SpyEye code.

32. Plaintiffs are informed and believe and thereupon allege that John Doe 29 goes by the alias "Donsft" and may be contacted at email address Donsft@hotmail.com. Upon information and belief, John Doe 29 is involved in purchasing and using the Zeus/SpyEye code.

33. Plaintiffs are informed and believe and thereupon allege that John Doe 30 goes by the alias "mary.j" and may be contacted at email address mary.j555@hotmail.com. Upon information and belief, John Doe 30 is involved in purchasing and using the Zeus/SpyEye code.

34. Plaintiffs are informed and believe and thereupon allege that John Doe 31 goes by the alias "susanneon" and may be contacted at email address susanneon@googlemail.com. Upon information and belief, John Doe 31 is involved in selling PDF exploits to deliver the Zeus/SpyEye code.

35. Plaintiffs are informed and believe and thereupon allege that John Doe 32 goes by the alias "kainhabe" and may be contacted at email address kainehabe@hotmail.com. Upon information and belief, John Doe 32 is involved in purchasing and using the Zeus/SpyEye code.

36. Plaintiffs are informed and believe and thereupon allege that John Doe 33 goes by the alias "virus_e_2003" and may be contacted at email address virus_e_2003@hotmail.com. Upon information and belief, John Doe 33 is involved in purchasing and using the Zeus/SpyEye code.

37. Plaintiffs are informed and believe and thereupon allege that John Doe 34 goes by the alias "spanishp" and may be contacted at email addresses spanishp@hotmail.com. Upon information and belief, John Doe 34 is involved in purchasing and using the Zeus/SpyEye code.

38. Plaintiffs are informed and believe and thereupon allege that John Doe 35 goes by the alias "sere.bro" and may be contacted at email address sere.bro@hotmail.com. Upon information and belief, John Doe 35 is involved in purchasing and using the Zeus/SpyEye code.

39. Plaintiffs are informed and believe and thereupon allege that John Doe 37 goes by the alias "vlad.dimitrov" and may be contacted at email address vlad.dimitrov@hotmail.com.

Upon information and belief, John Doe 37 is involved in purchasing and using the Zeus/SpyEye code.

40. Plaintiffs are informed and believe and thereupon allege that John Doe 38 goes by the alias "jheto2002" and may be contacted at email address jheto2002@gmail.com. Upon information and belief, John Doe 38 is involved in creating injection code to deliver the Zeus/SpyEye code.

41. Plaintiffs are informed and believe and thereupon allege that John Doe 39 goes by the alias "sector.exploits" and may be contacted at email address sector.exploits@gmail.com. Upon information and belief, John Doe 39 is involved in selling Adobe Flash exploit code to deliver the Zeus/SpyEye code.

42. Defendants own, operate, control, and maintain the Zeus Botnets through a command and control infrastructure hosted at and/or operating at the Harmful IP Domains and IP Addresses. The command and control infrastructure hosted and operated at the Harmful Domains and IP Addresses are maintained by the third-party domain registries, hosting companies and website providers set forth at Appendices A, B and C to this Complaint.

43. Plaintiffs are unaware of the true names and capacities of Defendants sued herein as John Does 1-21 and 25-39 inclusive and therefore sue these Defendants by such fictitious names. Plaintiffs will amend this complaint to allege Defendants' true names and capacities when ascertained. Plaintiffs will exercise due diligence to determine Defendants' true names, capacities, and contact information, and to effect service upon those Defendants.

44. Plaintiffs are informed and believe and therefore allege that each of the Defendants is responsible in some manner for the occurrences herein alleged, and that Plaintiffs' injuries and the injuries to Plaintiffs' customers and members herein alleged are proximately caused by such Defendants.

45. The actions and omissions alleged herein to have been undertaken by Defendants were undertaken by each Defendant individually, were actions and omissions that each Defendant authorized, controlled, directed, or had the ability to authorize, control or direct,

and/or were actions and omissions each Defendant assisted, participated in, or otherwise encouraged, and are actions for which each Defendant is liable. Each Defendant aided and abetted the actions of Defendants set forth below, in that each Defendant had knowledge of those actions and omissions, provided assistance and benefited from those actions and omissions, in whole or in part. Each Defendant was the agent of each of the remaining Defendants, and in doing the things hereinafter alleged, was acting within the course and scope of such agency and with the permission and consent of other Defendants.

JURISDICTION AND VENUE

46. This action arises out of Defendants' violation of the Federal Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125(a), (c)), and the Racketeer Influence and Corrupt Organizations Act (18 U.S.C. § 1962(c)). Therefore, the Court has subject matter jurisdiction over this action based on 28 U.S.C. § 1331. This is also an action for trespass to chattels, unjust enrichment, and conversion. This Court, accordingly, has subject matter jurisdiction under 28 U.S.C. § 1367.

47. Defendants have directed acts complained of herein toward the state of New York and the Eastern District of New York, have utilized instrumentalities located in New York and the Eastern District of New York to carry out the acts alleged in this Complaint, and engaged in other conduct availing themselves of the privilege of conducting business in New York and the Eastern District of New York.

48. In particular, Defendants control a network of compromised user computers called the "Zeus Botnets" that Defendants use to conduct illegal activities, thereby causing harm to the Plaintiffs as well as Plaintiffs' customers, members and the general public in the Eastern District of New York. Defendants have directed actions at the Eastern District of New York, by directing malicious computer code at computers of individual Internet users located in the Eastern District of New York, infecting those user computers with the malicious code and thereby making the user computers part of the Zeus Botnets. Figure 1 depicts the geographical

location of infected user computers in the Eastern District of New York from which Defendants sent spam email propagating the Zeus Botnets. Figure 2 depicts infected computers in the Eastern District of New York from which Defendants requested instructions from known Zeus Botnet command and control servers.

Figure 1 - *Computers In The Eastern District Of New York Propagating Zeus Botnet*

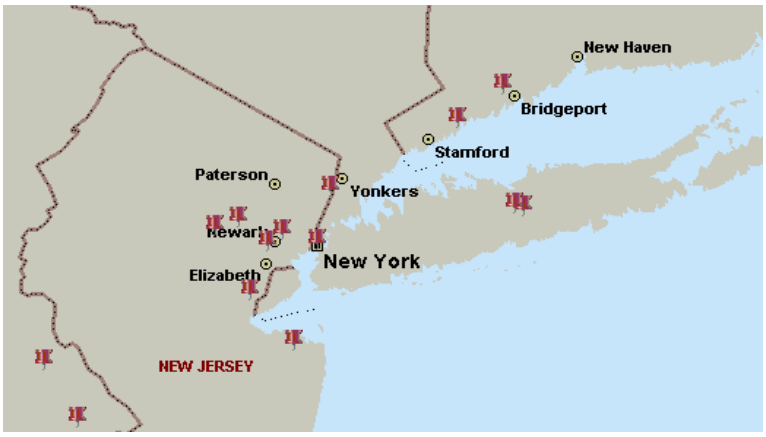
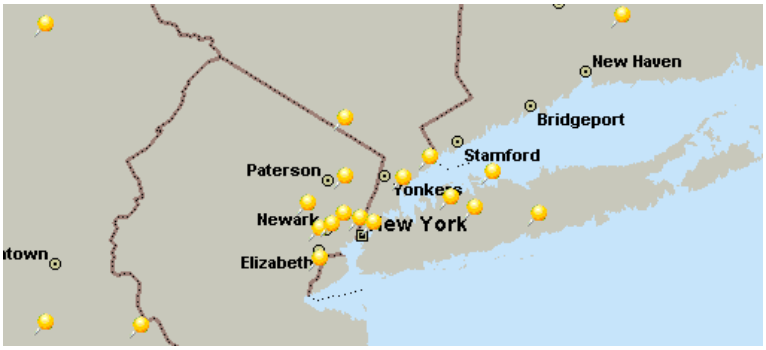


Figure 2 - *Zeus Botnet Computers In The Eastern District Of New York*



49. Defendants have undertaken the foregoing acts with knowledge that such acts would cause harm through user computers located in New York, thereby injuring Plaintiffs, their customers, members, and others in New York and elsewhere in the United States. Therefore, this Court has personal jurisdiction over Defendants.

50. Pursuant to 28 U.S.C. § 1391(b), venue is proper in this judicial district. A substantial part of the events or omissions giving rise to Plaintiffs' claims, together with a substantial part of the property that is the subject of Plaintiffs claims, are situated in this judicial district. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Defendants

are subject to personal jurisdiction in this judicial district.

51. Plaintiffs Microsoft and NACHA have been directly injured through the activities alleged herein and bring this action on their own behalf.

52. Plaintiff FS-ISAC's members are suffering immediate and threatened injury as a direct result of the activities alleged herein and there would be a justiciable controversy had the members brought suit themselves. FS-ISAC has associational standing as a representative of its members because (1) multiple FS-ISAC members would otherwise have standing to sue in their own right, (2) the interests the FS-ISAC association seeks to protect in this action are germane to the organization's purpose and (3) as FS-ISAC seeks only equitable relief, neither the claim asserted nor the relief requested requires participation of individual members in this action.

FACTUAL BACKGROUND

Plaintiffs' Products, Services And Reputation

53. Plaintiff Microsoft® is a provider of the Windows® operating system and the Outlook,® Hotmail®, Windows Live® and MSN® email and messaging services and a variety of other software and services. Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, establishing a strong brand and developing the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including the Microsoft®, Windows®, Outlook,® Hotmail®, Windows Live® and MSN® marks.

54. Plaintiff FS-ISAC is a trade organization compromised of 4,400 organizations including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, payment processors, and over 20 trade associations representing the majority of the U.S. financial services sector. It was established by the financial services sector in response to the

1998 Presidential Directive 63, later updated by the 2003 Homeland Security Presidential Directive 7, that requires that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the United States' critical infrastructure. (*See* www.fsisac.com/about/.) Its purpose is "to enhance the ability of the financial services sector to prepare for and respond to cyber and physical threats, vulnerabilities and interests...." FS-ISAC's activities include actively coordinating and promoting financial industry detection, analysis, and response to cyber security threats. FS-ISAC works closely with various government agencies including the U.S. Department of Treasury, Department of Homeland Security (DHS), Federal Reserve, Federal Financial Institutions Examination Council regulatory agencies, United States Secret Service, Federal Bureau of Investigation, National Security Agency, Central Intelligence Agency, and state and local governments. Financial institutions that are members of FS-ISAC have generated substantial goodwill with their customers, establishing a strong brand and developing their respective names and the names of their products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade.

55. Plaintiff NACHA manages the development, administration, and governance of the Automated Clearing House ("ACH") Network. The ACH is the backbone for the electronic movement of money and data. A critical part of NACHA's mission is to develop and implement a framework for risk management and network enforcement relating to the ACH Network. NACHA also provides resources to support and educate financial institutions and consumers regarding fraud and other forms of abuse of electronic payments systems. NACHA represents more than 10,000 financial institutions via 17 regional payment associations and direct membership. Due to its responsibilities, the high quality and effectiveness of its services and the expenditure of significant resources by NACHA to market its services, NACHA has generated substantial goodwill with its members and the public, establishing a strong name and the names of its services into strong and famous world-wide symbols that are well-recognized within its channels of trade.

56. Defendants, by operating, controlling, maintaining, and propagating the Zeus Botnets have caused and continue to cause severe and irreparable harm to each Plaintiff, their customers, their members, and the public at large.

Computer "Botnets"

57. In general, a "botnet" is a collection of individual computers running software that allows communication among those computers and that allows centralized or decentralized communication with other computers providing control instructions. A botnet network may be comprised of multiple, sometimes millions, of end-user computers infected with the malicious software ("malware" or "Trojan"). The individual computers in a botnet often belong to individual end-users who have unknowingly downloaded or been infected by such software that makes the computer part of the botnet. An end-user's computer may become part of a botnet when the user inadvertently interacts with a malicious website advertisement, clicks on a malicious email attachment, or downloads malicious software. In each such instance, software code is downloaded or executed on the user's computer, causing that computer to become part of the botnet, capable of sending and receiving communications, code, and instructions to or from other botnet computers.

58. Criminal organizations and individual cyber criminals often create, control, maintain, and propagate botnets in order to carry out misconduct that harms others' rights. They use botnets because of botnets' ability to support a wide range of illegal conduct, their resilience against attempts to disable them, and their ability to conceal the identities of the malefactors controlling them. The controllers of a botnet will use an infected end-user computer for a variety of illicit purposes, unknown to the end user. A computer in a botnet, for example, may be used to:

a. carry out theft of credentials and information, fraud, computer intrusions, or other misconduct;

b. anonymously send unsolicited bulk email without the knowledge or consent of the individual user who owns the compromised computer;

c. deliver further malicious software that infects other computers, making them part of the botnet as well; or

d. "proxy" or relay Internet communications originating from other computers, in order to obscure and conceal the true source of those communications.

Botnets provide a very efficient general means of controlling a huge number of computers and targeting any action internally against the contents of those computers or externally against any computer on the Internet.

59. Plaintiffs bring this action to stop Defendants from controlling, maintaining, and growing the Zeus Botnets that have caused harm to Plaintiffs, their customers and their members, and to the general public. Defendants control, maintain, and grow the Zeus Botnets through the command and control infrastructure hosted at and operated through the Harmful Domains and IP Addresses described herein and set forth at Appendices A, B and C.

The "Zeus Botnets"

60. The Zeus Botnets primarily carry out theft of account credentials for websites, particularly online banking websites. The Zeus Botnets' primary aim is to infect end-user computers in order to (1) steal the users' online account credentials, including online banking credentials, (2) access consumers' accounts with the stolen credentials, and (3) steal information from consumers' website accounts and steal funds from consumers' banking and financial accounts. The creators of the Zeus Botnets' malicious code, moreover, collaborate in a common operation to create, distribute, and operate the Zeus Botnets. The resulting harm to Plaintiffs, end-users, financial institutions, government agencies and the general public is the result of a single global criminal operation that controls, operates, and maintains the Zeus Botnets.

Defendants Work Together In A Common Operation To Create, Control, And Maintain The Zeus Botnets

61. The Zeus Botnets comprise a family of inter-related botnets – known on the Internet as the "Zeus", "Ice-IX," and "SpyEye" botnets. The "Zeus," "Ice-IX" and "SpyEye" botnets are built on the same software code and infrastructure. Defendant creators – whose

specific identities are currently unknown – have operated in anonymity on the Internet for several years.

62. The "Zeus" botnet code first emerged in 2007. The "Zeus" code evolved over time, becoming more sophisticated and including additional features designed to counter attempts to analyze and disable the botnet.

63. The "Ice-IX" code, which emerged in May 2011, is built on the "Zeus" code and contains enhancements to avoid virus-scanning software.

64. The "SpyEye" code was originally independent software, but in October 2010 was merged with the "Zeus" code and, from that point forward, "Zeus" code and functionality became part of the SpyEye code.

Defendants Offer Their Botnet Code For Sale

65. Defendants **John Doe 1, John Doe 2, and John Doe 3** have offered their botnet code for sale on the Internet as "builder kits" that allow others, including the other Defendants, to easily setup, operate, maintain, and propagate botnets to infect end-user computers, carry out financial theft, send spam email or engage in other malicious activities. Depending on the level of sophistication in particular versions, and the level of support and customization provided, the code may cost as little as $700 or up to $15,000 or more for more comprehensive or tailored versions. These kits contain software that enable other Defendants to generate executable botnet code, configuration files, and web server files that they deploy on command and control servers.

Defendants Work Together To Operate The Zeus Botnets

66. Plaintiffs are informed and believe and thereupon allege that the common code and characteristics of the Zeus, Ice-IX, and SpyEye botnets, and evidence regarding specific activities of the Defendants, demonstrate that the Zeus Botnets are controlled by a number of Defendants acting in concert. Upon information and belief, John Does 1-3, the creators of the botnet code, work together with the purchasers, developers and other sellers of the Zeus Botnet code in a continuous and coordinated manner to control, operate, distribute, and maintain the

Zeus Botnets. Upon information and belief, the malicious software that Defendants install on end-user machines all share common code and characteristics, and have evolved over time to more closely resemble one another. The three botnets are all available for sale on the same "underground" internet forums, and are all provided with similar tools and utilities.

67. John Does 4-39, Yevhen Kulibaba and Yuriy Konovalenko have individually or collectively purchased the Zeus Botnet code and, in concert with the creators of the code, are operating or otherwise facilitating the Zeus Botnets. Some of the defendants have specialized roles, including: (1) customizing the code, (2) creating "web inject" code, a delivery mechanism to introduce the botnet code onto victim computers, (3) recruiting "money mules" as intermediaries to create fraudulent bank accounts to which stolen funds are directed and withdrawn, and (4) acquiring domain names and IP addresses to host the command and control servers. The common characteristics of botnet code used by these Defendants indicate that they are controlled by the same group of Defendants, who are acting in concert. Plaintiffs' investigation reveals that the Defendant creators of the botnet code work together with these Defendant operators of the botnets in a continuous and coordinated manner to control, operate, distribute, and maintain the Zeus Botnets.

The Zeus Racketeering Enterprise

68. Upon information and belief, John Does 1-39, Yevhen Kulibaba and Yuriy Konovalenko constitute a group of persons associated together for a common purpose of engaging in a course of conduct, as part of an ongoing organization, with the various associates functioning as a continuing unit. The Defendants' enterprise has a purpose, with relationships among those associated with the enterprise, and longevity sufficient to permit those associates to pursue the enterprise's purpose. Upon information and belief, Defendants John Doe 1, John Doe 2, and John Doe 3 conspired to, and did, form an associated in fact enterprise (herein after the "Zeus Racketeering Enterprise") with a common purpose of developing and operating a global credential stealing botnet operation as set forth in detail herein.

69. The Zeus Racketeering Enterprise has existed since at least October of 2010, when John Doe 1 and John Doe 3 merged their respective botnet operations into a single, consolidated global credential stealing botnet. John Doe 2 joined and began participating in the Zeus Enterprise at an unknown date prior to fall of 2011. Other Defendants identified as John Does 4-39, Yevhen Kulibaba and Yuriy Konovalenko joined and began participating in the Zeus Enterprise at various times thereafter.

70. The Zeus Racketeering Enterprise has continuously and effectively carried out its purpose of developing and operating a global credential stealing botnet operation since that time, and will continue to do so absent the judicial relief that Plaintiffs request.

71. Both the purpose of the Zeus Racketeering Enterprise and the relationship between the Defendants is proven by: (1) the consolidation of the original Zeus botnet and the SpyEye botnet; (2) the subsequent development and operation of the enhanced Ice-IX botnet; and (3) Defendants' respective and interrelated roles in the sale, operation of, and profiting from the Zeus Botnets in furtherance of Defendants' common financial interests.

72. Upon information and belief, Defendants have conspired to, and have, conducted and participated in the operations of the Zeus Racketeering Enterprise through a continuous pattern of racketeering activity as set forth herein. Each predicate act is related to and in furtherance of the common unlawful purpose shared by the members of the Zeus Racketeering Enterprise. These acts are continuing and will continue unless and until this Court grants Plaintiffs' request for a temporary restraining order.

73. Upon information and belief, Defendants have conspired to, and have, knowingly and with intent to defraud trafficked in thousands of unauthorized access devices in the form of stolen passwords, bank account numbers and other account login credentials through the Zeus Botnets created and operated by Defendants.

74. As set forth in detail herein, Defendants have used the Zeus Botnets to steal, intercept and obtain this access device information from tens of thousands of individuals using

falsified web pages, and have then used these fraudulently obtained unauthorized access devices to steal millions of dollars from individuals' accounts.

75. Upon information and belief, Defendants have also conspired to, and have, knowingly and with intent to defraud, possessed, and do possess, thousands of such unauthorized access devices fraudulently obtained as described herein.

76. Upon information and belief, Defendants have conspired to, and have, knowingly and with intent to defraud, effected transactions with the stolen unauthorized access devices to receive millions of dollars in payment from individuals' bank accounts.

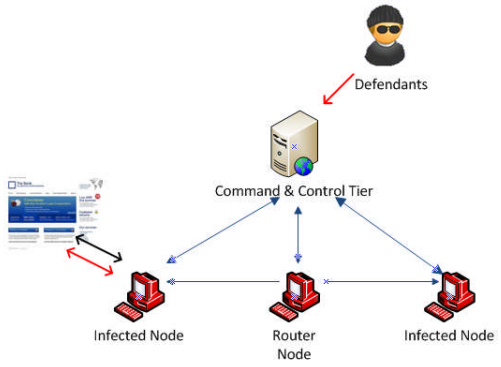
77. Upon information and belief, Defendants have conspired to, and have, executed a scheme to defraud scores of financial institutions by enabling members of the Zeus Racketeering Enterprise to fraudulently represent themselves as specific bank customers, thereby enabling them to access and steal funds from those customer accounts.

78. Upon information and belief, Defendants have further conspired to, and have, orchestrated the dispatch of "money mules" to the United States for the purpose of opening bank accounts using fraudulent identification documents, and then using these fraudulently obtained bank accounts, to receive and withdraw the funds stolen from legitimate bank customers.

79. Each of the foregoing illegal acts were conducted using interstate ACH and/or interstate and/or foreign wires as described herein, and therefore affected interstate and/or foreign commerce.

The Structure Of The Zeus Botnets

80. The Zeus Botnets are made up of two tiers of computers: an "Infected Tier," made up of computers infected with Zeus ("Infected Nodes"), some of which have been chosen by the botnet operator to perform additional tasks in managing the botnet ("Router Nodes"), and a "Command and Control Tier." This architecture facilitates the distribution of the botnet malware, propagation of the botnet, and obfuscation of the botnet controllers. The tiered architecture of the Zeus Botnets can generally be represented as follows:



81. The lowest tier—the Infected Tier—consists of millions of infected end-user computers, of the type commonly found in businesses, living rooms, schools, libraries, and Internet cafes around the world. The Infected Tier performs the botnets' daily illicit work. Owners of computers in the Infected Tier are targets of Defendants' theft of online credentials, personal information and money from these victims' bank accounts. Some computers in this tier, the "Router Nodes," are used in some versions of the Zeus Botnets as intermediary computers, relaying communications between different botnet computers and delivering commands and responses among botnet computers.

82. The highest level of the Zeus Botnets architecture—the "Command and Control Tier"—consists of specialized computers and/or software ("servers"). Defendants purchase and/or lease these servers to send commands to control the Zeus Botnets' end-user computers that make up the Infected Tier.

Defendants Use The Harmful Domains And IP Addresses To Infect And Control End-User Computers And To Steal Information And Money From Victims

83. Defendants rely on the Harmful Domains and IP Addresses to infect the end-users' computers, causing them to become part of the Zeus Botnets. Defendants may use software called a "Trojan downloader" that installs the malicious botnet software onto the end-user computer. The Defendants store this malicious software on computer servers at the Harmful Domains and IP Addresses. Defendants then mislead Internet users to visit these servers where the users unknowingly download the malicious software. The Harmful Domains and IP

Addresses that Defendants use to infect the Internet user computers are identified in Appendices A, B and C with the labels "Embedded_js," "Infector," "Source," "Dropzone," and "Updater."

84. Defendants' method of infection involves sending Internet users unwanted and unsolicited emails – "spam" emails. These spam emails contain links to one or more of the Harmful Domains and IP Addresses that contain the malicious botnet software. The content of the spam emails misleads Internet users to click on the links, causing the malicious software to be installed on the Internet users' computers without their knowledge or consent. Specifically, these spam emails falsely claim to be from Plaintiffs Microsoft, NACHA, financial institutions that are members of Plaintiff FS-ISAC, or from government agencies (such as the IRS), the American Bankers Association, or other companies. The spam emails contain those entities' trademarks and contain misleading messages to induce the user to click on malicious links.

85. Defendants have sent emails purporting to be from Plaintiff Microsoft offering a fake Microsoft "Critical Security Update" and a fake "Update for Microsoft Outlook/Outlook Express," requesting that users click a link. Defendants send spam emails purporting to be from NACHA requesting that the user click a link to purportedly manage a rejected ACH transaction. Other examples include emails:

a. purporting to originate from banks and requesting that users click to update their bank information;

b. purporting to be from the American Bankers Association and requesting that the user click on a link to view an account statement;

c. purporting to be from the IRS and requesting that the user click on a link to download a tax statement;

d. purporting to be from DHL or Federal Express and requesting that the user click on a link to confirm a delivery;

e. purporting to be an electronic greeting card, inviting users to click on a link to view the card; and

f. purporting to be from social media websites, such as Facebook or others, requesting that users click on a link to accept invitations from "friends."

86. The links in these emails, when clicked, direct the user to one of the Harmful Domains and IP Addresses, and result in the infection of the user's computer with the malicious

software. Defendants send a very large volume of such spam. The monthly averages for spam emails propagating the Zeus Botnets and infringing NACHA's trademarks alone are in the range of one hundred million. At one point in August 2011, such spam emails infringing NACHA's trademarks were as high as 167 million emails in a 24 hour period. By contrast, the normal volume for authentic outbound email messages from NACHA is only 1,500 emails per day.

87. Defendants also use many of the Harmful Domains and IP Addresses to collect stolen financial account credentials and other confidential information from infected end-user computers. Once account credentials are stolen, they are transferred over the Internet from the Zeus Botnet software on the victim computers to Defendants at the computers associated with these Harmful Domains and IP Addresses. Defendants then use this account information to log into victims' accounts and initiate transfers of information or funds from victims' online accounts into accounts controlled by Defendants. The Harmful Domains and IP Addresses that Defendants use to collect stolen information and account credentials are identified in Appendices A, B and C with the label "Dropzone."

88. Defendants use certain of the Harmful Domains and IP Addresses (identified with the label "Infector," "Source" or "Updater" in Appendices A, B and C) to deliver initial or new configurations and target lists to end-user computers. These domains and IP addresses enable the Defendants to control the infected end-user computers once the end-user computers have been infected with the malicious botnet software. These Harmful Domains and IP Addresses house the Zeus Botnets' "configuration" files.

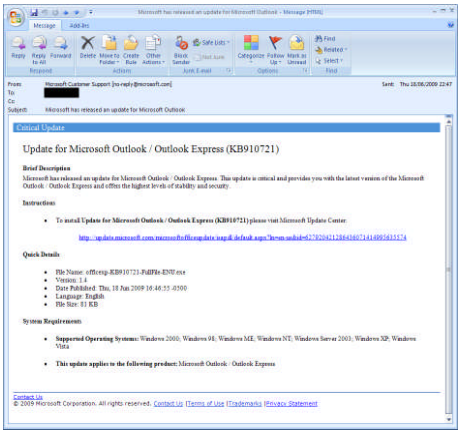
89. The "configuration" files stored at the Harmful Domains and IP Addresses contain templates that mimic the websites of virtually all major financial institutions. Defendants have designed these website templates to contain not only the trademarks of major financial institutions, but also identical copies of those financial institutes' website content. Most Internet users are unable to tell the difference between a financial institution's genuine website and the website templates used by the Zeus Botnets.

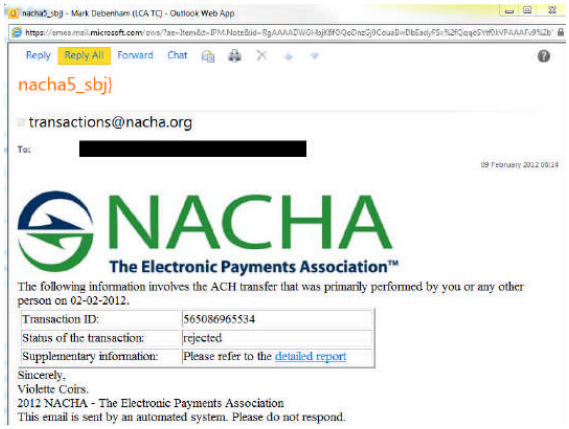
90. The website templates are sent from the Harmful Domains and IP Addresses to

infected end-user computers, and when the end-users attempt to access and use their online banking or other websites, the website templates are presented instead of the genuine website. The end-users believe that they have accessed their online banking website and input their banking credentials (*e.g.*, name, address, account number, password, social security number, and other identifying information) into the website. In fact, the Zeus Botnets have intercepted the end-user's banking credentials. The "configuration" files also contain the domain names and IP addresses to which the stolen information is to be sent back.

91. The computers at the Harmful Domains and IP Addresses also contain "spam-templates" or resource files that are delivered from the Harmful Domains and IP Addresses to infected end-user computers. The malicious software on the infected end-user computers use these templates to generate spam email that is then sent either from email accounts accessed from the end-user computers, or sent directly from those computers. The spam is intended to infect other end-user computers and to grow the Zeus Botnets. These spam templates and resource files contain the trademarks of Microsoft, NACHA, American Bankers Association, and FS-ISAC member institutions.

92. The spam templates and resource files also contain other content and messages designed to deceive Internet users into believing that a spam email is actually coming from Microsoft, NACHA, American Bankers Association, or FS-ISAC member institutions, in order to mislead email recipients into clicking links in the email. The following are examples of Defendants' infringement of Microsoft's and NACHA's trademarks:


Update for Microsoft Outlook / Outlook Express (KB910721)


nacha5_sbj

transactions@nacha.org

NACHA
The Electronic Payments Association™

The following information involves the ACH transfer that was primarily performed by you or any other person on 02-02-2012.

Transaction ID:	565086965534
Status of the transaction:	rejected
Supplementary information:	Please refer to the detailed report

Sincerely,
Violette Coirs.
2012 NACHA - The Electronic Payments Association
This email is sent by an automated system. Please do not respond.

93. Defendants' website templates and spam templates stored on the Harmful Domains and IP Addresses contain counterfeit copies of the trademarks of Microsoft, NACHA, American Bankers Association, and FS-ISAC member institutions, such as those reflected above.

Defendants Use The Harmful IP Domains And IP Addresses To Access End-Users' Computers Without Authorization

94. Internet users whose computers are infected with the Zeus Botnets' malicious software are damaged by changes that the Zeus Botnets make to the Windows operating system software, altering the normal and approved settings and functions, destabilizing the system, and forcibly drafting customers' computers into the botnet. Once installed on an end-user's computer, the Botnets' malicious software makes changes at the deepest and most sensitive levels of the computer's operating system. The software installs, intercepts and takes unauthorized control of normal Windows processes. The software alters the behavior of various Windows routines by manipulating registry key settings. The software replaces Windows files with files of the same name that contain the malicious software.

95. Once the Zeus Botnets' malicious software infects an end-user computer, it turns the infected computer into the worker of the botnet, performing the day-to-day illegal activity. The malicious code instructs the infected end-user computer to, among other things: (a) hide the malware, (b) lower security settings, (c) contact the command and control servers to retrieve a "configuration file" containing instructions, including website templates that mimic the websites and trademarks of Plaintiffs, financial institutions or other companies, (d) in connection with other software, generate spam email that infringe Plaintiffs' and others' trademarks, (e) steal usernames, passwords, and other credentials from the victim, (f) communicate stolen data back to the command and control servers, (f) intercept or carry out transactions without the user's knowledge or consent.

96. Upon information and belief, Microsoft's customers are usually unaware that their computers are infected and have become part of the Zeus Botnets. Upon information and belief,

even if they are aware of the infection, Microsoft's customers often lack the technical resources or skills to resolve the problem, allowing their computers to be misused indefinitely. Even with professional assistance, cleaning an infected end-user computer can be exceedingly difficult, time-consuming, and frustrating.

Defendants Use The Harmful Domains And IP Addresses To Steal End-Users' Banking Credentials and Personal Information

97. The Zeus Botnets cause injury to Plaintiffs Microsoft, NACHA, and FS-ISAC as well as Plaintiffs' customers and members when the Zeus Botnets steal infected end-users' online banking credentials and personal information.

98. Once installed on an end-user computer, the malware detects when an Internet user navigates to any website specified in the configuration files, particularly online banking websites. Defendants have specified websites ending in ".microsoft.com/," Microsoft's "hotmail.com" or "live.com" email websites, and a variety of online banking sites as targets. For example, when a user visits their online banking website, the malicious software may do one of the following:

a. Access the real banking website, but unknown to the user, execute instructions that modify or extend the website. In particular, the Zeus Botnets may cause the website to display extra fields into which users are instructed to type additional sensitive information that is not requested at the legitimate website. For example, the fake versions of the websites may seek information such as ATM "PIN," social security number, mother's maiden name, addresses, birthdates and similar information.

b. Intercept the request from the user's web browser and present the user with a fake website, based on the template, which appears to be the legitimate website; or

c. Intercept the request and redirect the user to a different fake website that appears to be the legitimate website.

99. The websites of nearly every major financial institution, Microsoft and a wide array of other Internet companies have been targeted by the Defendants and the Zeus Botnets in this way. In each case, the website presented to the user is a fake or modified version, which

appears very similar to the legitimate website and misuses the trademarks and website content of financial institutions, Microsoft and others.

100. When an Internet user enters his or her account credentials at these websites—*e.g.*, username, password and other additional personal data—the Defendants' malicious software collects this data and transmits it over the Internet to command and control servers operated at the Harmful Domains and IP Addresses. The Zeus Botnets' code is also able to: (1) inject Defendants' own transactions into a victim's online banking session and (2) divert funds from a victim's banking account via wire or ACH transaction to an account controlled by Defendants.

101. Defendants use the victims' account credentials to access victims' online financial or other accounts and steal money and information from such accounts. Defendants often hire "money mules"—individuals who travel to different countries, including the United States—in order to set up bank accounts to receive transfers of stolen funds from the victims' accounts. The money mules withdraw funds from the accounts they have set up, keep a percentage for their own payment and transmit the remainder to the Defendants.

102. The malware is specifically designed to allow Defendants to perpetrate this malicious activity without revealing any evidence of the fraud until it is too late for the user or owners of these websites to regain control over funds or stolen information. For example, the software can re-write on-screen account balances, generate false account statements, hide transactions from the user's view and hide itself from antivirus software.

Defendants Use The Harmful Domains And IP Addresses To Send Bulk "Spam" Email

103. Defendants, through the Zeus Botnets and often in connection with other software, also send, without the user's knowledge or permission, unsolicited bulk email (often known as "spam"). The spam email usually contains links to malicious code that infects further computers adding them to the botnets. The spam may be sent from victims' email accounts that Defendants have taken control of using the botnets. Defendants may also send spam email

directly from infected end-user computers.

104. In either situation, the configuration files containing spam templates are retrieved from the command and control servers operating through the Harmful Domains and IP Addresses and downloaded to infected computers, or other computers used to access victim email accounts without authorization. These spam templates work with the email server software to structure the appearance and content of the outgoing spam email messages. As shown in examples reproduced above, the spam templates and resource files contain the trademarks of Microsoft, NACHA and other content designed to mislead the recipients of the spam email into clicking on links in the spam email.

Defendants And The Zeus Botnets Severely Injure Microsoft, NACHA and FS-ISAC's Financial Institution Members

105. Microsoft is the provider of the Windows operating system, Hotmail email services, and a variety of other software and services. It has invested substantial resources developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, and has developed its name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including the "Microsoft," "Outlook" and "Windows" marks. Microsoft's trademark registrations are attached as Appendix D to this Complaint.

106. NACHA is a non-profit association which manages the development, administration, and governance of the ACH Network, the backbone for the electronic movement of money and data. NACHA represents more than 10,000 financial institutions via 17 regional payments associations and direct membership. NACHA has developed goodwill with financial institutions, merchants and individual customers and has established NACHA's name as a strong brand in connection with secure, reliable electronic transactions. NACHA has

registered trademarks representing the quality of its services and brand, including "NACHA," "NACHA – The Electronic Payment Association" and the NACHA logo. NACHA's trademark registrations are attached as Appendix E to this Complaint.

107. FS-ISAC is a non-profit organization, funded entirely by its members, primarily larger financial services firms, and represents the interests of the financial services sector and financial institution members against cyber and physical threats and risk. FS-ISAC and its financial institution members have made significant investments in developing high-quality, secure online banking and financial services platforms, promoting consumer confidence in those systems and protecting financial institutions and consumers from abuse related to these systems. FS-ISAC's members have invested in developing their brands, trademarks and trade names in association with the financial services they offer. Attached as Appendix F to this Complaint are representative trademark registrations of FS-ISAC's members injured by the Zeus Botnets.

108. As a provider of online e-mail services such as Hotmail, Microsoft must maintain spam filters to stop spam from the Zeus Botnets from reaching customers. Microsoft's Hotmail systems are the target of a substantial volume of spam from and promoting the Zeus Botnets. The sending of vast amounts of spam email to Microsoft's Hotmail email services imposes a burden on Microsoft's servers, and requires Microsoft to expend substantial resources in an attempt to defend against and mitigate the effects of this vast amount of spam email.

109. The spam infringes trademarks of Microsoft, NACHA and FS-ISAC's financial institution members, thus confusing consumers and deceiving them into installing malicious software. Consumers who have been deceived often become angry or frustrated at Microsoft and NACHA, incorrectly believing them to be responsible for the spam email. Plaintiffs must expend resources attempting to remediate consumer confusion and responding to such confusion. For example, in merely a one year period, NACHA had to expend $624,000 of its limited resources to combating spam abuse and consumer confusion.

110. The websites of Microsoft and FS-ISAC's financial institution members are directly targeted by Defendants and the Zeus Botnets. Defendants steal credentials to access those websites, enabling them to steal personal information from Microsoft users and steal funds from FS-ISAC's financial institution members and their customers. Conservatively, since 2007, the Defendants and the Zeus Botnets have stolen $100 million from victims whose online financial accounts are taken over by Defendants.

111. The Zeus Botnets also make use of counterfeit copies of the trademarks of FS-ISAC's members and Microsoft, including the trade names, logos and website content of those companies, in order to deceive users into inputting their confidential account information. Such activity causes injury to FS-ISAC member institutions and Microsoft by causing consumer confusion and diminishing their brands and goodwill.

112. Further, Microsoft, as a provider of the Windows operating system and Internet Explorer web browser, must incorporate security features in an attempt to stop account credential theft by the Zeus Botnets from occurring to customers using Microsoft's software. In general, the abuse of Microsoft's, NACHA's and FS-ISAC's members' trademarks to defraud consumers in this way injures the Plaintiffs.

113. Microsoft devotes significant computing and human resources to combating infections by the Zeus Botnets and helping customers determine whether or not their computers are infected and, if so, cleaning them. For example, since 2007 Microsoft has detected 13 million computers infected with some version of the Zeus Botnets. Microsoft has had to expend substantial resources researching the Zeus Botnet software, developing anti-virus filters to combat the Zeus Botnets, responding to consumer complaints and assisting consumers in cleaning their machines, and investigating and prosecuting enforcement action against the Zeus Botnets.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF
Violation of the Computer Fraud & Abuse Act, 18 U.S.C. § 1030

(Microsoft and FS-ISAC)

114. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 113 above.

115. Defendants (1) knowingly and intentionally accessed Microsoft's and FS-ISAC's financial institution members' protected computers, (2) knowingly and intentionally accessed Microsoft's customers' protected computers and Plaintiffs' protected computers, and (3) accessed such protected computers without authorization or in excess of any authorization and knowingly caused the transmission of a program, information, code and commands, and as a result of such conduct intentionally caused damage without authorization to the protected computers (18 U.S.C. § 1030(a)(5)(A)), and; intentionally accessed the protected computers without authorization, and as a result of such conduct caused damage and loss (18 U.S.C. § 1030(a)(5)(C)).

116. Defendants' conduct has caused a loss to Microsoft and FS-ISAC's financial institution members during a one-year period aggregating at least $5,000.

117. Plaintiffs Microsoft and FS-ISAC's financial institution members have suffered damages resulting from Defendants' conduct.

118. Plaintiff Microsoft seeks injunctive relief and compensatory and punitive damages under 18 U.S.C. §1030(g) in an amount to be proven at trial.

119. Plaintiff FS-ISAC seeks injunctive relief.

120. As a direct result of Defendants' actions, Plaintiffs Microsoft and FS-ISAC's financial institution members have suffered and continue to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SECOND CLAIM FOR RELIEF
Violation of CAN-SPAM Act, 15 U.S.C. § 7704
(Microsoft)

121. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 113 above.

122. Plaintiff Microsoft is a provider of Internet access service. Microsoft enables users to access content, including proprietary content, electronic mail, and other Internet services.

123. Defendants initiated the transmission of unsolicited bulk spam e-mail, which are commercial electronic messages, via the Zeus Botnets, through Microsoft's customers' computers and through Microsoft's computers, which are used in interstate and foreign commerce and communication, to thousands or millions of computers, which are also used in interstate and foreign commerce and communication and are "protected computers" as defined by 18 U.S.C. § 1030(e)(2)(B).

124. By sending messages via the Zeus Botnets, Defendants initiated the transmission of commercial electronic mail messages to protected computers that contained materially false or misleading header information in violation of 15 U.S.C. § 7704(a)(1).

125. Defendants initiated the transmission of commercial electronic messages to protected computers with actual or fairly implied knowledge that the subject headings of the messages would likely materially mislead recipients regarding the contents or subject matter of the message in violation of 15 U.S.C. § 7704(a)(2).

126. Defendants transmitted to protected computers commercial e-mail messages that did not contain a functioning return electronic mail address or other Internet-based mechanism that recipients could use to contact Defendants and indicate their desire to opt-out of future messages from Defendants, in violation of 15 U.S.C. § 7704(a)(3).

127. Defendants initiated the transmission to protected computers of commercial electronic messages that did not provide: (a) clear and conspicuous identification that the message was an advertisement or solicitation; (b) clear and conspicuous notice of the right to decline to receive future messages; or (c) a valid physical postal address of the sender, in violation of 15 U.S.C. § 7704(a)(5).

128. Defendants' unsolicited bulk e-mails were sent as part of a systematic pattern and practice that did not conspicuously display a return electronic mail address by which the

recipients could submit to the true sender a reply requesting that no further commercial e-mails be sent to the recipient.

129. As a direct result of Defendants' actions, Microsoft has suffered harm in an amount to be determined at trial.

130. Microsoft is entitled to the greater of actual damages or statutory damages in accordance with 15 U.S.C. § 7706(g)(1)(B).

131. On information and belief, Defendants' actions were willful and knowing, entitling Microsoft to aggravated damages in accordance with 15 U.S.C. § 7706(g)(3)(C).

132. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

THIRD CLAIM FOR RELIEF
Violation Of Electronic Communications Privacy Act, 18 U.S.C. § 2701
(Microsoft and FS-ISAC)

133. Plaintiffs reallege and incorporate by reference the allegations contained in paragraphs 1 through 113 above.

134. Microsoft's and Microsoft's customers' computers and servers and its licensed operating system are facilities through which electronic communication service is provided to its users and customers.

135. The computers and servers of FS-ISAC's financial institution members are facilities through which electronic communication service is provided to its users and customers.

136. Defendants knowingly and intentionally accessed the computers and servers of Microsoft, Microsoft's customers' and FS-ISAC's financial institution members without authorization or in excess of any authorization granted by Plaintiffs.

137. Through this unauthorized access, Defendants had access to, obtained and altered, and/or prevented legitimate, authorized access to wire electronic communications, including but not limited to electronic communications while they were in electronic storage in the computers

and servers of Microsoft, Microsoft's customers and FS-ISAC's financial institution members.

138. Plaintiff Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

139. Plaintiff FS-ISAC seeks injunctive relief.

140. As a direct result of Defendants' actions, Microsoft and FS-ISAC's financial institution members have suffered and continue to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

FOURTH CLAIM FOR RELIEF
Trademark Infringement Under the Lanham Act – 15 U.S.C. § 1114 *et. seq.*
(Microsoft, NACHA, FS-ISAC)

141. Plaintiffs reallege and incorporate by this reference each and every allegation set forth in paragraphs 1 through 113 above.

142. Defendants have used Microsoft's, NACHA's and FS-ISAC's financial institution members' trademarks in interstate commerce.

143. The Zeus Botnets generate and use counterfeit copies of Microsoft's, NACHA's and FS-ISAC's financial institution members' trademarks in fake websites and in spam email, including through the software operating from and through the Command and Control Servers operating at the Harmful Domains and IP Addresses. By doing so, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake websites and spam e-mail and material promoted through the fake websites and spam e-mail.

144. By using Microsoft's, NACHA's and FS-ISAC's financial institution members' trademarks falsely in connection with spam e-mail and fake websites, Defendants have caused, and are likely to cause, confusion, mistake, or deception as to the origin, sponsorship, or approval of the e-mail and fake websites generated and disseminated by the Zeus Botnets. By doing so, Defendants have caused, and are likely to cause, confusion, mistake, or deception as to the origin, sponsorship, or approval of the conduct, actions, products and services carried out by or promoted by Defendants and the Zeus Botnets.

145. As a result of their wrongful conduct, Defendants are liable to Plaintiffs for violation of this provision of the Lanham Act.

146. Plaintiffs Microsoft and NACHA seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

147. Plaintiff FS-ISAC seeks injunctive relief.

148. As a direct result of Defendants' actions, Microsoft, NACHA and FS-ISAC's financial institution members have suffered and continue to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

149. Defendants' wrongful and unauthorized use of Microsoft's, NACHA's and FS-ISAC's financial institution members' trademarks to promote, market, or sell products and services constitutes trademark infringement pursuant to 15 U.S.C. § 1114 *et seq*.

FIFTH CLAIM FOR RELIEF
False Designation of Origin Under The Lanham Act – 15 U.S.C. § 1125(a)
(Microsoft, NACHA, FS-ISAC)

150. Plaintiffs reallege and incorporate by this reference each and every allegation set forth in paragraphs 1 through 113 above.

151. Microsoft's, NACHA's and FS-ISAC's financial institution members' trademarks are distinctive marks that are associated with Microsoft, NACHA and FS-ISAC's financial institution members and exclusively identify their businesses, products, and services.

152. The Defendants, through the Zeus Botnets, make unauthorized use of Microsoft's, NACHA's and FS-ISAC's financial institution members' trademarks. The Zeus Botnets generate and use counterfeit copies of Microsoft's, NACHA's and FS-ISAC's financial institution members' trademarks in fake websites and in spam email, including through the software operating from and through the Command and Control Servers operating at the Harmful Domains and IP Addresses. By doing so, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake websites and spam e-mail and

material promoted through the fake websites and spam e-mail.

153. By using Microsoft's, NACHA's and FS-ISAC's financial institution members' trademarks falsely in connection with spam e-mail and fake websites, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the e-mail and fake websites generated and disseminated by the Zeus Botnets. By doing so, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the conduct, actions, products and services carried out by or promoted by Defendants and the Zeus Botnets.

154. As a result of their wrongful conduct, Defendants are liable to Plaintiffs for violation of the Lanham Act, 15 U.S.C. § 1125(a).

155. Plaintiffs Microsoft and NACHA seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

156. Plaintiff FS-ISAC seeks injunctive relief.

157. As a direct result of Defendants' actions, Microsoft, NACHA and FS-ISAC's financial institution members have suffered and continue to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SIXTH CLAIM FOR RELIEF
Trademark Dilution Under The Lanham Act – 15 U.S.C. § 1125(c)
(Microsoft, NACHA, FS-ISAC)

158. Plaintiffs reallege and incorporate by this reference each and every allegation set forth in paragraphs 1 through 113 above.

159. Microsoft's, NACHA's and FS-ISAC's financial institution members' trademarks are distinctive marks that are associated with Microsoft, NACHA and FS-ISAC's financial institution members and exclusively identify their businesses, products, and services.

160. The Zeus Botnets makes unauthorized use of Microsoft's, NACHA's and FS-ISAC's financial institution members' trademarks. By doing so, Defendants are likely to cause

dilution by blurring and dilution by tarnishment of the Plaintiffs' Marks and the Marks of Plaintiffs' members.

161. Plaintiffs Microsoft and NACHA seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

162. Plaintiff FS-ISAC seeks injunctive relief.

163. As a direct result of Defendants' actions, Microsoft, NACHA and FS-ISAC's financial institution members have suffered and continue to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SEVENTH CLAIM FOR RELIEF
Violations of the Racketeer Influenced and Corrupt Organizations Act (RICO) – 18 U.S.C. § 1962(c)
(Microsoft, NACHA)

164. Plaintiffs reallege and incorporate by this reference each and every allegation set forth in paragraphs 1 through 113 above.

165. Beginning in or before October of 2010 and continuing up through the filing of this Complaint, Defendants John Doe 1 and John Doe 3 were and are associated in fact with the Zeus Racketeering Enterprise and have conducted its affairs through a pattern of racketeering activity, with such conduct and activities affecting interstate and foreign commerce. At various dates thereafter and continuing through the filing of this Complaint, Defendants John Doe 2 and John Does 4-39, Yevhen Kulibaba and Yuriy Konovalenko also became associated in fact with the Zeus Racketeering Enterprise and have also conducted and participated in its affairs through a pattern of racketeering activity that affects interstate and foreign commerce. Defendants have engaged in an unlawful pattern of racketeering activity involving thousands of predicate acts of wire fraud, 18 U.S.C. § 1343, bank fraud, 18 U.S.C. § 1344, and fraud and related activity in connection with access devices. 18 U.S.C. § 1029.

166. The members of the Zeus Racketeering Enterprise share the common purpose of developing and operating a global credential stealing botnet operation as set forth in detail above.

167. Defendants have knowingly and with intent to defraud trafficked in thousands of unauthorized access devices in the form of stolen passwords, bank account numbers and other account login credentials through the Zeus Botnets created and operated by Defendants. As set forth in detail above, Defendants have used the Zeus Botnets to steal, intercept and obtain this access device information from thousands of individuals using falsified web pages, and have then used these fraudulently obtained unauthorized access devices to steal millions of dollars from these individuals' accounts, all in violation of 18 U.S.C. § 1029(a)(2).

168. Defendants have also knowingly and with intent to defraud, possessed, and do possess, thousands of unauthorized access devices fraudulently obtained as described above, in violation of 18 U.S.C. § 1029(a)(3).

169. Defendants have also knowingly and with intent to defraud effected transactions with stolen unauthorized access devices to receive millions of dollars in payment from individuals' bank accounts, in violation of 18 U.S.C. § 1029(a)(7).

170. Also as set forth in detail above, Defendants have executed a scheme to defraud scores of financial institutions by enabling members of the Zeus Enterprise to fraudulently represent themselves as bank customers, thereby enabling them to access and steal funds from those customer accounts. Defendants have further orchestrated the dispatch of "money mules" to the United States for the purpose of opening bank accounts using fraudulent identification documents, and then using these fraudulently obtained bank accounts to receive and withdraw the funds stolen from the bank's legitimate customers, all in violation of 18 U.S.C. § 1344.

171. Each of the violations of 18 U.S.C. §1029(a) and 18 U.S.C. § 1344 described above were conducted using internet communications "transmitted by means of wire … in interstate or foreign commerce," in violation of 18 U.S.C. § 1343.

172. Microsoft and NACHA have been and continue to be directly injured by Defendants' conduct. But-for the alleged pattern of racketeering activity, Microsoft and NACHA would not have incurred damages.

173. Plaintiffs Microsoft and NACHA seek injunctive relief and compensatory and

punitive damages in an amount to be proven at trial.

EIGHTH CLAIM FOR RELIEF
Conspiracy to Violate the Racketeer Influenced and Corrupt Organizations Act (RICO) – 18 U.S.C. § 1962(d)
(Microsoft, NACHA)

174. Plaintiffs reallege and incorporate by this reference each and every allegation set forth in paragraphs 1 through 113 above.

175. Beginning in or before October of 2010 and continuing up through the filing of this Complaint, Defendants John Does 1-39, Yevhen Kulibaba and Yuriy Konovalenko conspired to associate in fact with the Zeus Racketeering Enterprise and conduct its affairs through a pattern of racketeering activity, with such conduct and activities affecting interstate and foreign commerce. Defendants further conspired to engage in an unlawful pattern of racketeering activity involving thousands of predicate acts of wire fraud, 18 U.S.C. § 1343, bank fraud, 18 U.S.C. § 1344, and fraud and related activity in connection with access devices. 18 U.S.C. § 1029.

176. The members of the Zeus Racketeering Enterprise conspired for the common purpose of developing and operating a global credential stealing botnet operation as set forth in detail above.

177. Microsoft and NACHA have been and continue to be directly injured by Defendants' conduct. But-for the alleged conspiracy to conduct a pattern of racketeering activity, Microsoft and NACHA would not have incurred damages.

178. Plaintiffs Microsoft and NACHA seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

NINTH CLAIM FOR RELIEF
Common Law Trespass to Chattels
(Microsoft, FS-ISAC)

179. Plaintiffs reallege and incorporate by this reference each and every allegation set forth in paragraphs 1 through 113 above.

180. Defendants' actions in operating the Zeus Botnets result in unauthorized access to

the computers of Microsoft, Microsoft's customers and FS-ISAC's financial institution members and result in unauthorized intrusion into those computers, theft of information, account credentials and funds, and unsolicited, bulk electronic mail being sent to, from or through the computers of Microsoft, Microsoft's customers and FS-ISAC's financial institution members.

181. Upon information and belief, Defendants intentionally caused this conduct and this conduct was unauthorized.

182. Defendants' actions have caused injury to Microsoft, Microsoft's customers and FS-ISAC's financial institution members and imposed costs on Microsoft, Microsoft's customers and FS-ISAC's financial institution members, including time, money and a burden on the computers of Microsoft, Microsoft's customers and FS-ISAC's financial institution members. Defendants' actions have caused injury to Microsoft's and FS-ISAC's financial institution members' business goodwill and have diminished the value of Microsoft's and FS-ISAC's financial institution members' possessory interest in their computers and software.

183. Plaintiff Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

184. Plaintiff FS-ISAC seeks injunctive relief.

185. As a direct result of Defendants' actions, Microsoft and FS-ISAC's financial institution members have suffered and continue to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

TENTH CLAIM FOR RELIEF
Conversion
(Microsoft, FS-ISAC)

186. Plaintiffs reallege and incorporate by this reference each and every allegation set forth in paragraphs 1 through 113 above.

187. Defendants have willfully interfered with and converted the personal property of Microsoft, Microsoft's customers and FS-ISAC's financial institution members, without lawful justification, as a result of which Microsoft, Microsoft's customers and FS-ISAC's financial

institution members have been deprived of possession and use of their property.

188. Plaintiff Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

189. Plaintiff FS-ISAC seeks injunctive relief.

190. As a direct result of Defendants' actions, Microsoft and FS-ISAC's financial institution members have suffered and continue to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

ELEVENTH CLAIM FOR RELIEF

Unjust Enrichment
(Microsoft, FS-ISAC, NACHA)

191. Plaintiffs reallege and incorporate by this reference each and every allegation set forth in paragraphs 1 through 113 above.

192. The acts of Defendants complained of herein constitute unjust enrichment of the Defendants at Plaintiffs' expense in violation of the common law.

193. Defendants accessed, without authorization, computers running Microsoft's and FS-ISAC's financial institution members' software or computers which otherwise belong to those Plaintiffs.

194. Defendants used, without authorization or license, the facilities of Microsoft's and FS-ISAC's financial institution members' software and computers which belong to those Plaintiffs to, among other acts, deliver malicious software, steal personal information, account credentials and money, support the Zeus Botnets, infringe the trademarks of Microsoft, NACHA and FS-ISAC's financial institution members, deliver unsolicited, bulk e-mail and deceive users.

195. Defendants' actions in operating the Zeus Botnets result in unauthorized access to the computers of Microsoft, Microsoft's customers and FS-ISAC's financial institution members and result in delivery of malicious software, theft of personal information, account credentials and money, support of the Zeus Botnets, infringement of the trademarks of Microsoft, NACHA and FS-ISAC's financial institution members, delivery of unsolicited bulk e-mail and deception

of users.

196. Defendants profited unjustly from their unauthorized and unlicensed use of Plaintiffs' software, computers, and/or intellectual property.

197. Upon information and belief, Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized and unlicensed use of software, computers and/or intellectual property of Plaintiffs.

198. Retention by the Defendants of the profits they derived from their unauthorized and unlicensed use of software, computers and/or intellectual property of Plaintiffs would be inequitable.

199. Defendants' unauthorized and unlicensed use of Plaintiffs' software, computers and/or intellectual property have damaged Microsoft, NACHA and FS-ISAC's financial institution members.

200. Plaintiffs Microsoft and NACHA seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial, and Defendants should disgorge their ill-gotten profits.

201. Plaintiff FS-ISAC seeks injunctive relief.

202. As a direct result of Defendants' actions, Microsoft, NACHA and FS-ISAC's financial institution members have suffered and continue to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs prays that the Court:

1. Enter judgment in favor of Plaintiffs and against the Defendants.

2. Declare that Defendants' conduct has been willful and that Defendants have acted with fraud, malice and oppression.

3. Enter a preliminary and permanent injunction enjoining Defendants and their

officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein.

4. Enter a preliminary and permanent injunction isolating and securing the botnet infrastructure, including the software operating from and through the Harmful Domains and IP Addresses and placing that infrastructure outside of the control of Defendants or their representatives or agents.

5. Enter judgment awarding Plaintiffs Microsoft and NACHA actual damages from Defendants adequate to compensate Microsoft and NACHA for Defendants' activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial.

6. Enter judgment in favor of Plaintiffs Microsoft and NACHA, disgorging Defendants' profits.

7. Enter judgment in favor of Plaintiffs Microsoft and NACHA, awarding enhanced, exemplary and special damages, in an amount to be proved at trial.

8. Enter judgment in favor of Plaintiffs Microsoft, NACHA and FS-ISAC awarding attorneys' fees and costs, and;

9. Order such other relief that the Court deems just and reasonable.

Dated: June 29, 2012

Respectfully Submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

By: s/ Richard A. Jacobsen
Richard A. Jacobsen
51 West 52nd Street
New York, NY 10019

Tel: (212) 506-5000
Fax: (212) 506-5151
Attorneys for Plaintiffs
Microsoft Corporation
National Automated Clearing House Association
FS-ISAC, Inc.